LA-UR-01-6915

Approved for public release; distribution is unlimited.

Title: A HIERARCHICAL MODEL FOR ESTIMATING COMPLEX SYSTEM RELIABILITY

Author(s): V. Johnson, D-1
T. Graves, D-1
M. Hamada, D-1
C. S. Reese, D-1

Submitted to: Seventh Valencia International Meeting on Bayesian Statistics, June 2-6, 2002, Tenerife, Spain

Los Alamos
NATIONAL LABORATORY

A Hierarchical Model for Estimating the Reliability of Complex Systems

Valen E. Johnson, Todd L. Graves, Michael Hamada, and C. Shane Reese
Statistical Sciences Group
Los Alamos National Laboratory

December 20, 2001

Abstract

We describe a model for assessing the reliability of complex systems comprised of multiple components. Components of the system are assumed to be linked together through a known reliability diagram (i.e., a fault tree). Both serial and parallel configurations of subcomponents are permitted. Novel features of this model are the natural manner in which failure data collected at either the component or subcomponent level can be incorporated into the posterior distribution and the pooling of failure information across similar subcomponents within the same or related systems. An example involving the performance of an anti-aircraft missile defense system is used to illustrate the methodology.

1 Background

In estimating the reliability of a complex system, it often happens that test data and prior expert opinion are available at system, subsystem, and component levels. Methodology for combining these various sources of information in a consistent fashion has proven problematic, and the goal of this article is the description of a Bayesian heirarchical model that resolves this difficulty. For simplicity, we restrict discussion to systems in which components or subcomponents may be regarded as either functional or not. Extensions to more general situations are briefly examined at the end of the article.

To provide context, it is useful to begin with a review of related research in Bayesian system reliability. Most relevant to the model considered here are the papers by Martz, Waller and Fickas (1988) and Martz and Waller (1990), where complex systems, comprised of series and parallel subcomponents, were modeled using beta priors and binomial likelihoods at component, subsystem and system levels. Within this framework, an "induced" higher-level prior was obtained by propagating lower-level posteriors up through the system fault diagram, and combining these posteriors with "native" higher-level priors to obtain an "induced" prior at the next system level. These "induced" priors were approximated by beta distributions using a methods-of-moments type procedure. The combination of native priors and posterior distributions obtained from lower-level system data, both of which were expressed as beta distributions, was accomplished by expressing the resulting induced priors as a beta distributions with parameters representing a weighted average of the constituent beta densities. This process was propogated through higher and higher system levels until an approximation to the joint posterior distribution on the total system reliability was obtained.

Many reliability models do not consider prior expert opinion and data at multiple system levels. Springer and Thompson (1966, 1969), and Tang, Tang and Moskowitz (1994, 1997) provide exact or approximated system reliability distributions obtained by propagating the component posteriors through the system structure. Thompson and Chang (1975), Chang and Thompson (1976), Lampkin and Winterbottom (1983) and Winterbottom (1994) use approximations for exponential lifetimes rather than binomial data. Others propose methods for evaluating or bounding moments of the system reliability posterior distribution (Cole (1975), Mastran (1976), Dostal and Iannuzzelli (1977), Mastran and Singpurwalla (1978), Barlow (1985), Natvig and Eide (1987), Soman and Misra (1993)). These moments can also be used in the beta approximations employed by Martz, Waller and Fickas (1988) and Martz and Waller (1990). Soman and Misra (1993) proposed a distributional approximation based on a maximum entropy principle.

Numerous models have, of course, also been proposed for modeling non-binomial data. Thompson and Chang (1975), Chang and Thompson (1976), Mastran (1976), Mastran and Singpurwalla (1978), Lampkin and Winterbottom (1983), and Winterbottom (1994) consider models for exponential lifetime data. Hulting and Robinson (1990, 1994) examine Weibull models. Poisson count data, where the number of units failing in a specified period, are discussed by Hulting and Robinson (1990), Sharma and Bhutani (1992), Hulting and Robinson (1994), Sharma and Bhutani (1994), and Martz and Baggerly (1997). Currit and Singpurwalla (1988) and Bergman and Ringi (1997a) consider dependence of components due to a common operating environment. Bergman and Ringi (1997b) incorporate data from non-identical environments.

Bier (1994) addresses the issue of aggregation error. Specifically, a logical difficulty arises when combining prior information data at distinct component levels. Bier asserts that there are basically two mechanisms available for overcoming this difficulty: (1) update component priors with component data and propagate up to get a system posterior, or (2) propagate component priors up to a system prior and update with system data to get system posterior. Unfortunately, these two methods yield distinct solutions. In the methodology introduced in this paper, we remedy the disparate solutions.

In Section 2 we introduce a Bayesian hierarchical modeling approach to estimation of system reliability. In Section 3 the computational algorthms used in estimation are proposed. The application of our approach to an anti-aircraft missile problem is presented in Section 4. We discuss the methodology and present future research possibilities in Section 5.

2 Methodology

To illustrate the model proposed here, consider Figure 1, which depicts a fault tree for an anti-aircraft missile system. The general features illustrated in this figure include the composition of a system by multiple subsystems, and the composition of these subsystems by further subsystems and components. In general, binomial data and prior expert opinion will be available at different system levels, and our goals in modeling such systems are to evaluate the probability that a missile drawn at random from the stockpile population functions, to provide stockpile managers with information regarding the necessity for conducting full-system tests–which can be very expensive–to evaluate this probability, and to identify subsystems for which additional data might best be collected to improve estimation of overall system reliability.

Four sources of data are considered here. The first is data collected from actual component or subsystem tests and is here assumed to take the form of binomial observations. In degradation models, the age of the component at the time of the test may also be available. Next, expert opinion regarding the probability that a specific component or subsystem fails may be available. A third, less precise source of information is expert opinion stating that a group of components in a given system or in related systems have similar failure probabilities. For example, in the missile system depicted above, an expert may assert that the reliability of the missile battery is "similar" to the reliability of a battery in a related missile system, or that reliabilities of the eject and flight motors are similar. However, the expert may not have knowledge regarding the specific probability that any component within a group of similar components functions. Finally, we wish to model the fact that "terminal nodes" (i.e., com-

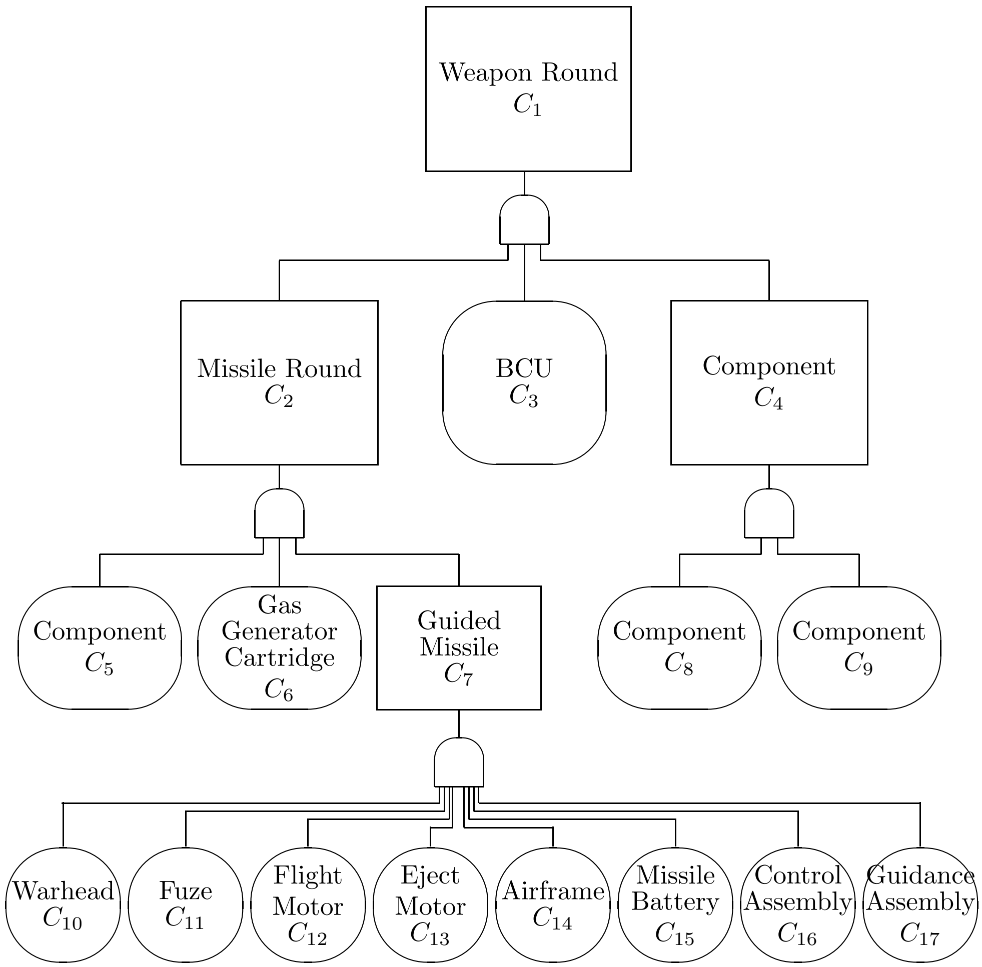

Figure 1: *Reliability Fault Tree Diagram for Missile Reliability*

ponents at the bottom of the fault tree having no subcomponents themselves) may also be grouped into sets of comparably reliable components without the guidance of actual expert opinion.

To model these four sources of information, we first assume that the failure probabilities of components in distinct branches of the fault tree are conditionally independent given their unknown success probabilities, and that the success of the system requires successful functioning of all components. Extensions to systems that include redundant components or in which component failures are not independent are discussed in the summary. Nodes in the reliability diagram are labeled C_i, where i indicates the component or subcomponent index. The function $a_{(i)}$ provides the "parent" component (or system) containing (sub)component i, while $g(i, m)$ indicates the group of components that expert m asserts have similar failure rates. We let p_i denote the probability that component C_i functions when the missile is fired. The set of components for which test data is available is denoted by S_0, and within this set x_i denotes the number of times component i functioned successfully in n_i trials. For simplicity of exposition, aging effects are not considered, making a simple binomial likelihood appropriate for modeling (x_i, n_i).

The incorporation of expert opinion can play a potentially important role in assessing the reliability of the system as a whole, particularly in large complex systems for which data collected on individual subcomponents may be sparse. Furthermore, expert opinion may be available from several experts, and the quality of information obtained from each expert may vary. To model expert opinion, we therefore assume that the prior density obtained from expert m concerning a specific value of p_i takes the form of a beta density, and let the set of combinations of (i, m) for which expert opinion is available be denoted by S_1. More specifically, we assume that the net contribution in the joint posterior density arising from such prior information is

$$\frac{\Gamma(N_m + 2)}{\Gamma(N_m\pi_{i,m} + 1)\Gamma[N_m(1 - \pi_{i,m}) + 1]} p_i^{N_m\pi_{i,m}} (1 - p_i)^{N_m(1-\pi_{i,m})} \equiv \mathrm{B}(p_i\, ;\, N_m\pi_{i,m} + 1, N_m(1 - \pi_{i,m}) + 1). \quad (1)$$

In (1), $\pi_{i,m}$ represents expert m's point estimate of p_i, and N_m represents the precision of expert m. For concreteness, we assume that each expert precision parameter N_m is drawn from a gamma density with known parameters α_m and β_m, parameterized here as

$$\mathrm{G}(N_m\, ;\, \alpha_m, \beta_m) = \frac{\beta_m^{\alpha_m}}{\Gamma(\alpha_m)} N_m^{\alpha_m - 1} \exp(-\beta_m N_m). \quad (2)$$

Note that expert opinion is assumed to take the form of a binomial likelihood with a maximum at $\pi_{i,m}$ – this convention eliminates the possibility that the joint density specified on all model parameters is improper, and also implicitly handles the aggregation problem identified by Bier (1994) by simply treating expert opinion has "data."

When prior information regarding component success probabilities is unknown, but expert groupings of components are available, (1) is augmented by assuming that $\pi_{i,m}$ is replaced by $\rho_{m,g}$, where $\rho_{m,g}$ represents the common, but unknown, success probability assigned by expert m to components in group g (i.e., components for which $g(i, m) = g$). The contribution to the joint posterior distribution on model parameters from such information is assumed to take the form

$$\prod_{(i,m)\in S_2} \mathrm{B}(p_i\, ;\, K_m\rho_{m,g} + 1, K_m(1 - \rho_{m,g}) + 1). \quad (3)$$

Here, S_2 denotes the combinations of (i, m) for which such grouping information is available.

As in (1), the parameter K_m is assumed to be drawn *a priori* from a gamma density having parameters ζ_m and η_m. The prior success parameter $\rho_{m,g}$ is assumed to be drawn from a beta density with known parameters $\delta_{g,m}$ and $\epsilon_{g,m}$, respectively.

Finally, for leaves in the fault tree a hierarchical prior specification may be obtained by further assuming that each terminal node's success probability is drawn from a beta density with parameters $J_0 \varrho_0$ and $J_0(1-\varrho_0)$. The set of terminal nodes in denoted by S_3.

For notational simplicity, we assume that all terminal nodes are, *a priori*, exchangeable, but this restriction may be relaxed by using expert judgment to group the terminal nodes in a manner similar to that used in the specification of (3). In that case, J_0 and ϱ_0 would be subscripted with the appropriate prior group. The parameter J_0 is assumed drawn from a gamma density with parameters τ_0 and ϕ_0; ϱ_0 is assumed *a priori* to be drawn from a beta density with parameters ψ_0 and ω_0.

As discussed in the previous section, combining data and prior information at different levels within a reliability diagram has often proven problematic, both from the perspectives of computational tractability and model consistency. Our solution to this conundrum is to simply re-express non-terminal node probabilities in terms of terminal node probabilities using deterministic relations derived from an examination of the system reliability diagram. For example, from Figure 1, it is evident that the probability that the guided missile functions, p_7, is equal to the product of the probabilities that the warhead (p_{10}), fuze (p_{11}), flight motor (p_{12}), eject motor (p_{13}), airframe (p_{14}), missile battery (p_{15}), control assembly (p_{16}), and guidance assembly(p_{17}) all function. Thus,

$$p_7 = \prod_{i=10}^{17} p_i \tag{4}$$

and, for example, the prior specification on p_7 is interpreted as a prior specification on this product:

$$\begin{aligned} f_{7,m}(p_7 \mid \pi_{7,m}, K_m) &\equiv f_{7,m}(\prod_{i=10}^{17} p_i \mid \pi_{7,m}, N_m) && (5) \\ &\propto \left[\prod_{i=10}^{17} p_i\right]^{N_m \pi_{7,m}} \left[1 - \prod_{i=10}^{17} p_i\right]^{N_m(1-\pi_{7,m})}. && (6) \end{aligned}$$

Note that variable substitutions based on the reliability diagram do not uniquely identify a joint distribution on the terminal node probabilities, in this case p_{10} through p_{17}. However, together with the assumption that the distributions of these probabilities are defined with respect to Lesbesque measure on the unit interval and given the hierarchical specification, such substitutions do yield a uniquely defined joint distribution on these parameters.

Combining these assumptions leads to a joint posterior distribution on all model parameters proportional to

$$
\begin{aligned}
&[\boldsymbol{p}, \mathbf{N}, \boldsymbol{\rho}, \mathbf{K}, \boldsymbol{\varrho}, \mathbf{J} \mid \mathbf{x}, \mathbf{n}, \boldsymbol{\pi}, \boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\zeta}, \boldsymbol{\eta}, \boldsymbol{\delta}, \boldsymbol{\epsilon}, \boldsymbol{\tau}, \boldsymbol{\phi}, \boldsymbol{\psi}, \boldsymbol{\omega}] \propto \\
&\quad \times \prod_{i \in S_0} p_i^{x_i}(1-p_i)^{n_i} \times \prod_{m:\exists(i,m)\in S_2} \mathrm{G}(K_m\,;\,\zeta_m, \eta_m) \\
&\quad \times \prod_{(i,m)\in S_1} \mathrm{B}(p_i\,;\,N_m\pi_{i,m}+1, N_m(1-\pi_{i,m})+1) && (7) \\
&\quad \times \prod_{(i,m)\in S_2} \mathrm{B}(p_i\,;\,K_m\rho_{m,g}+1, K_m(1-\rho_{m,g})+1) && (8) \\
&\quad \times \prod_{i\in S_3} \mathrm{B}(p_i\,;\,J_0\varrho_0, J_0(1-\varrho_0)+1) && (9) \\
&\quad \times \prod_{m:\exists(i,m)\in S_2} \mathrm{B}(\rho_{m,g}\,;\,\delta_m, \epsilon_m) \times \mathrm{B}(\varrho_0\,;\,\psi_0, \omega_0) \\
&\quad \times \mathrm{G}(J_0\,;\,\tau_0, \psi_0) \times \prod_{m:\exists(i,m)\in S_1} \mathrm{G}(N_m\,;\,\alpha_m, \beta_m). && (10)
\end{aligned}
$$

In this expression, values of non-terminal node probabilities are assumed to be expressed in terms of the appropriate functions of terminal node probabilities, as defined from the system fault tree.

An examination of the contributions to the joint posterior distribution arising from the three types of prior information (7–9) reveal obvious similarities, but there are also important distinctions between these parameterizations. For example, in (7), the value of N_m represents the precision of the expert's opinion, while in (8) and (9), K_m and J_0 describe the similarity of items reliabilities within a grouping.

2.1 Hierarchical prior model

The hierarchical prior model on the terminal node probabilities plays a crucial role in rendering estimates of the overall system reliability insensitive to the level of detail included in the system fault diagram. As an illustration of this point, consider a simple system comprised of three components, and suppose that a single binomial observation with 4 successes and 1 failure is observed at the system level. Then without a hierarchical specification on the component probabilities and under the model assumptions stated above, the posterior distribution on the system reliability would be proportional to

$$(p_2p_3p_4)^4(1-p_2p_3p_4) \qquad (11)$$

where the system reliability, p_1, is assumed equal to $p_2p_3p_4$.

With the implied uniform distribution on p_2-p_4, the posterior mean of p_1 in this model is 0.507. Note that the posterior mean on p_1 (with a uniform prior) is .714 when the system is not decomposed into subsystems. And, of course, this bias becomes more severe as the number of subcomponents in the system increases.

In contrast, the hierarchical prior specification on p_2-p_4 with $\psi_0 = \omega_0 = 0.5$ results in a posterior mean of 0.718 for p_1, while the same specification with $\psi_0 = \omega_0 = 1.0$ results in a posterior mean of 0.687. Both results are relatively insensitive to the number of subcomponents specied for the system.

3 Estimation strategies

The joint distribution on model parameters specied in (10) does not lend itself to analytical evaluation of the system or component reliabilities. However, a componentwise Metropolis-Hastings algorithm can be implemented in relatively straightforward way. In our version of such a scheme, we used a random-walk Metropolis-Hastings algorithm with Gaussian proposal densities specified on the logistic scale for the terminal node probabilities, for ϱ_0 and for $\rho_{m,g}$. Precision parameters were similarly updated using a random-walk Metropolis-Hastings scheme with Gaussian increments specified on the logarithmic scale. The resulting Metropolis-Hastings algorithms was implemented using a general-purpose Java MCMC system developed at Los Alamos National Laboratory. (Graves, 2001).

4 Analysis of anti-aircraft missile data

Anti-aircraft missiles are intended to provide defense from attacking enemy aircraft. Anti-aircraft missiles take on many forms, some being launched from the ground and others launched from the air, and yet others launched from the decks of ships. The United States has over 15 different anti-aircraft missiles in its current arsenal. In each case there are stockpiles of these weapons, of varying sizes, which are stored in the event of certain types of conflicts. One important consideration in these stockpiles is the probability that a randomly selected unit will perform its intended task to success. This probability can be framed in terms of a reliability problem.

These weapons are made up of several components as well as several subsystems. An example of components and subsystems that make up a generic anti-aircraft missile system is shown in Figure 1. Associated with that system are sources of data. Some of these sources include component tests, subsystem tests, and full system tests. In our example, we had 45 observations on components $C_4, C_5, C_6, C_{11}, C_{12}, C_{13}, C_{15}$ and C_{16}. We also had 126 observations on C_3, and the bulk of our data, over 1400 observations, were available at the full system level ($C_{1,0,1}$). At each of components $C_2, C_7, C_8, C_9, C_{10}, C_{14}$, and C_{17}, no data were collected.

After discussions with experts on this system, reliability classes were formed as shown in Figure 1. That is, the reliability classes are indicated by the levels in the reliability fault tree. Thus, components 10-17 form one class, components 5-9 form another class, and components 2-4 form a class. These classes form the basis for the hierarchical model on the component reliabilities.

One important consideration for this problem is the uncertainty in reliability estimates when no data are collected at the full system level. Therefore, our results present two cases: the case with full system data included and the case with no full system tests.

Applying the model discussed in Section 2, we obtained the reliability posterior distributions for each of the components and the expert precision parameter. The system reliability posterior distributions with the system data included and system data excluded are plotted in Figure 2. We note the agreement between the two posterior distributions (full system tests included vs. full system tests excluded). In every case, the 95% HPD region includes essentially the entire distribution with full system information included. The scales from these plots have been removed due to classification concerns, but they not extend to the interval $(0, 1)$. Also of interest is the posterior distribution for the expert precision (N_m). The posterior mean for this distribution is 12.2. This indicates that the expert's opinion is worth approximately 12 full system tests. Given the prior mean of 5, we conclude that the expert was reasonably well calibrated with the system structure and data.

5 Conclusions

The proposed hierarchical model offers several advantages over existing models for system reliabilities. Among these are the ease of including diverse sources of information at different levels of the system into the model for overall system reliabilities, a coherent framework for incorporating multiple sources of prior expert opinion through the treatment of expert opinion

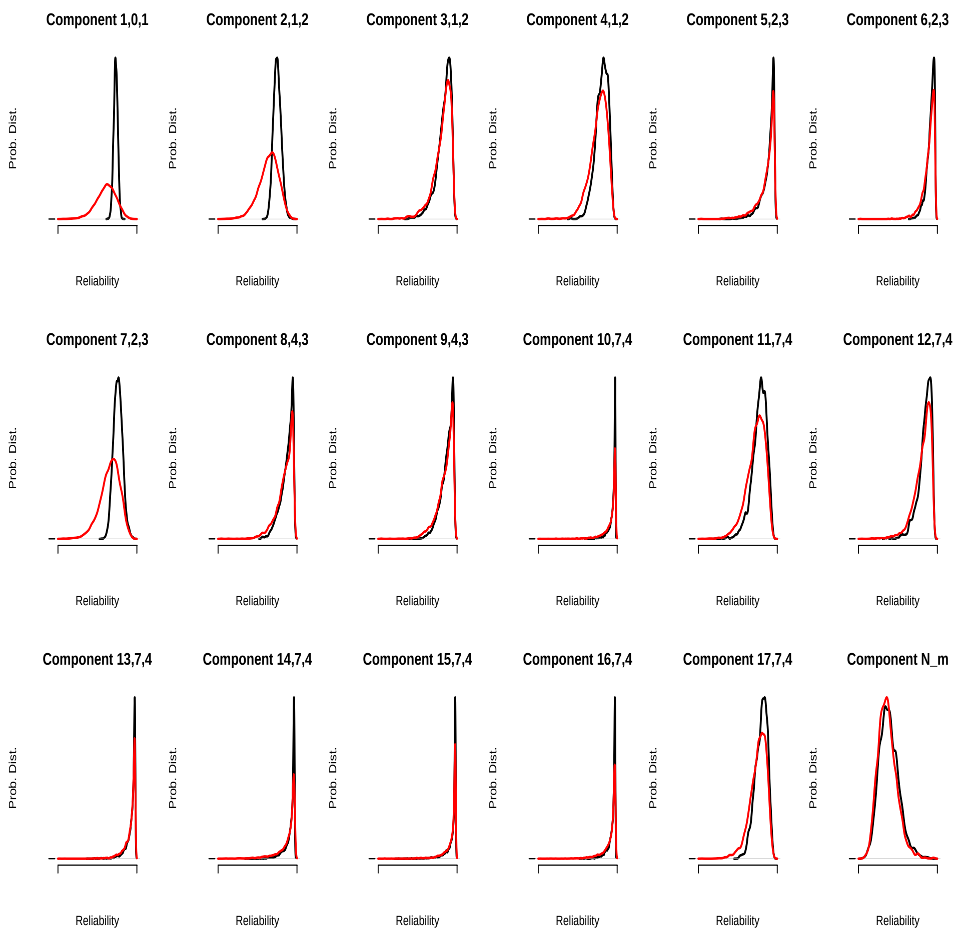

Figure 2: Posterior distributions for the reliability of the system represented in Figure 1. The black lines were based on the model that included the full-system flight tests and the dashed lines using only system level data.

as (imprecisely-observed) data, and the natural elimination of aggregation errors through the definition of non-terminal probabilities using the assumed structure of the system fault tree and terminal node probabilities.

A simplistic form of our hierarchical model for reliability was described in this paper. In future work we plan to extend this framework to include non-serial systems and to incorporate degradation models for component reliabilities. Other outstanding issues include the development of diagnostics to assess the adequacy of the system diagram in describing the functioning of the system, and the introduction of models for dependencies between subcomponents within subsystems.

6 References

Barlow, R.E. (1985) "Combining Component and System Information in System Reliability Calculation," in *Probabilistic Methods in the Mechanics of Solids and Structures*, Eds. S. Eggwertz and N.L. Lind, Springer-Verlag, Berlin, 375-383.

Bergman, B. and Ringi, M. (1997a), "Bayesian System Reliability Prediction," *Scandinavian Journal of Statistics*, 24, 137-143.

Bergman, B. and Ringi, M. (1997b), "System Reliability Prediction Using Data from Non-identical Environments," *Reliability Engineering and System Safety*, 58, 183-190.

Bier, V.M. (1994), "On the Concept of Perfect Aggregation in Bayesian Estimation," *Reliability Engineering and System Safety*, 46, 271-281.

Chang, E.Y. and Thompson, W.E. (1976), "Bayes Analysis of Reliability of Complex Systems," *Operations Research*, 24, 156-168.

Cole, P.V.Z. (1975), "A Bayesian Reliability Assessment of Complex Systems for Binomial Sampling," *IEEE Transactions on Reliability*, R-24, 114-117.

Currit, A. and Singpurwalla, N.D. (1988), "On the Reliability Function of a System of Components Sharing a Common Environment," *Journal of Applied Probability*, 26, 763-771.

Dostal, R.G. and Iannuzzelli, L.M. (1977), "Confidence Limits for System Reliability When Testing Takes Place at the Component Level," in *The Theory and Applications of Reliability* (Vol. 2), Academic Press, New York, 531-552.

Graves, T.L. (2001), "YADAS: An Object-Oriented Framework for Data Analysis Using Markov Chain Monte Carlo," Los Alamos National Laboratory Technical Report, LA-UR-01-4804.

Hulting, F.L. and Robinson, J.A. (1990), "A Bayesian Approach to System Reliability," Research Publication No. GMR-7110, General Motors Research Laboratories, Warren, MI.

Hulting, F.L. and Robinson, J.A. (1994), "The Reliability of a Series System of Repairable Subsystems: A Bayesian Approach," *Naval Research Logistics*, 41, 483-506.

Lampkin, H. and Winterbottom, A. (1983), "Approximate Bayesian Intervals for the Reliability of Series Systems from Mixed Subsystem Test Data,", *Naval Research Logistics*, 30, 313-317.

Lynn, N., Singpurwalla, N. and Smith, A. (1998), "Bayesian Assessment of Network Reliability," *Siam Review*, 40, 202-227.

Martz, H.F. and Baggerly, K.A. (1997), "Bayesian Reliability Analysis of High-Reliability Systems of Binomial and Poisson Subsystems," *International Journal of Reliability, Quality and Safety Engineering*, 4, 283-307.

Martz, H.F. and Waller, R.A. (1990), "Bayesian Reliability Analysis of Complex Series/Parallel Systems of Binomial Subsystems and Components," *Technometrics*, 32, 407-416.

Martz, H.F., Waller, R.A. and Fickas, E.T. (1988), "Bayesian Reliability Analysis of Series Systems of Binomial Subsystems and Components," *Technometrics*, 30, 143-154.

Mastran, D.V. (1976), "Incorporating Component and System Test Data Into the Same Assessment: A Bayesian Approach," *Operations Research*, 24, 491-499.

Mastran, D.V. and Singpurwalla, N.D. (1978), "A Bayesian Estimation of the Reliability of Coherent Structures," *Operations Research*, 26, 663-672.

Natvig, B. and Eide, H. (1987), "Bayesian Estimation of System Reliability," *Scandinavian Journal of Statistics*, 14, 319-327.

Sharma, K.K. and Bhutani, R.K. (1994), "Bayesian Reliability Analysis of a Parallel System," *Microelectronics Reliability*, 34, 761-763.

Sharma, K.K. and Bhutani, R.K. (1992), "Bayesian Reliability Analysis of a Series System," *Reliability Engineering and System Safety*, 53, 227-230.

Soman, K.P. and Misra, K.B. (1993), "On Bayesian Estimation of System Reliability," *Microelectronics Reliability*, 33, 1455-1459.

Springer, M.D. and Thompson, W.E. (1966), "Bayesian Confidence Limits for the Product of N Binomial Parameters," *Biometrika*, 53, 611-613.

Springer, M.D. and Thompson, W.E. (1969), "Bayesian Confidence Limits for System Reliability," in *Proceedings of the 1969 Annual Reliability and Maintainability Symposium*, Institute of Electrical and Electronics Engineers, New York, 515-523.

Tang, J., Tang, K. and Moskowitz, H. (1994), "Bayes Credibility Intervals for Reliability of Series Systems with Very Reliable Components," *IEEE Transactions on Reliability*, 43, 132-137.

Tang, J., Tang, K. and Moskowitz, H. (1997), "Exact Bayesian Estimation of System Reliability from Component Test Data," *Naval Research Logistics*, 44, 127-146.

Thompson, W.E. and Chang, E.Y. (1975), "Bayes Confidence Limits for Reliability of Redundant Systems," *Technometrics*, 17, 89-93.

Winterbottom, A. (1984), "The Interval Estimation of System Reliability from Component Test Data," *Operations Research*, 32, 628-640.